23. fejezet – Az IPv6 protokoll

Az IPv6 protokoll

Az IPv6 protokoll tervezésének és megjelenésének fő szempontja az IPv4 protokoll lecserélése volt, amire az IPv4 ismert korlátai miatt volt szükség. Az első IPv6-tal kapcsolatos szabványok 1992. év végére készültek el, és egy evolúció során további hét változatból 1994-re született meg a ma IPv6-nak nevezett protokoll, amelyet 1994. november 17-én az Internet Engineering Steering Group (IESG) is elfogadott és felhasználásra javasolt. Az IPv6 protokoll leírását az RFC2460 dokumentum tartalmazza. 2011. június 8-ára ismert tartalomszolgáltatók, mint a Google, a Facebook és a Yahoo világméretű tesztnapot kezdeményeztek, "World IPv6 Day", azaz az IPv6-világnap néven.
A protokoll tervezésekor nemcsak az IPv4 hibáit igyekeztek megszüntetni, hanem új szolgáltatásokat is bele kívántak építeni, amelyek gyorsabbá és az új felhasználói igényeknek jobban megfelelővé teszik.
Az IPv6 az IPv4 szerves folytatása. Sem a TCP, az UDP, a DNS, (ezek később kerülnek részletesen ismertetésre) sem az egyéb alkalmazói protokollok nem változnak, csupán maga az IP, amely viszont továbbra is megmarad megbízhatatlan szolgáltatást nyújtó datagram hálózatnak. Az egyetlen lényeges változás az architektúrában az, hogy az ARP funkciót többé nem külön definiáljuk minden kapcsolat típushoz, hanem maga az IP tartalmazza szomszéd felismerő protokoll (NDP – Neighbour Discovery Protocol) néven. Az egész protokollcsaládban általános lett a változó hosszúságú opciók beillesztésének lehetősége, melyek mindig egy hossz, egy típus és egy adatmezőből állnak, valamint minden esetben meghatározzák, hogy mit kell tenni a fel nem ismert opciókkal. Így egy későbbi bővítés esetén is biztosan tudhatjuk azt, hogy a régi berendezéseink hogyan viselkednek az új környezetben.

Az IPv6 protokoll megalkotásakor a következő célokat tűzték ki, és próbáltak elérni.

1. Támogatni kell az eddiginél (IPv4) sokkal több hosztot, lehetőleg milliárdos nagyságrendben. A kioszthatók hosztok száma fontosabb, mint a hatékony címtartomány hozzárendelés.
2. Csökkenteni kell az útválasztók táblázatainak méretét.
3. A több hoszt miatt mindenképpen gyorsítani kell az útválasztókban a csomagok feldolgozását. Ehhez a protokoll egyszerűsítésére van szükség.
4. Támogatni kell az eddiginél (IPv4) sokkal jobb biztonságot, hitelesítést és titkosítást.
5. Kiemelt figyelmet kell fordítani a valós idejű szolgáltatásokra.
6. A többesküldés (Multicast) hatékonnyá tétele hatósugár megadásával.

7. Lehetővé kell tenni a hosztok barangolását anélkül, hogy IPv6 címük eközben megváltozna.
8. A protokollnak képesnek kell lenni a további fejlődésre.
9. Meg kell engedni, hogy a régi és az új protokoll akár évekig képes legyen egymás mellett létezni, egymás zavarása nélkül.

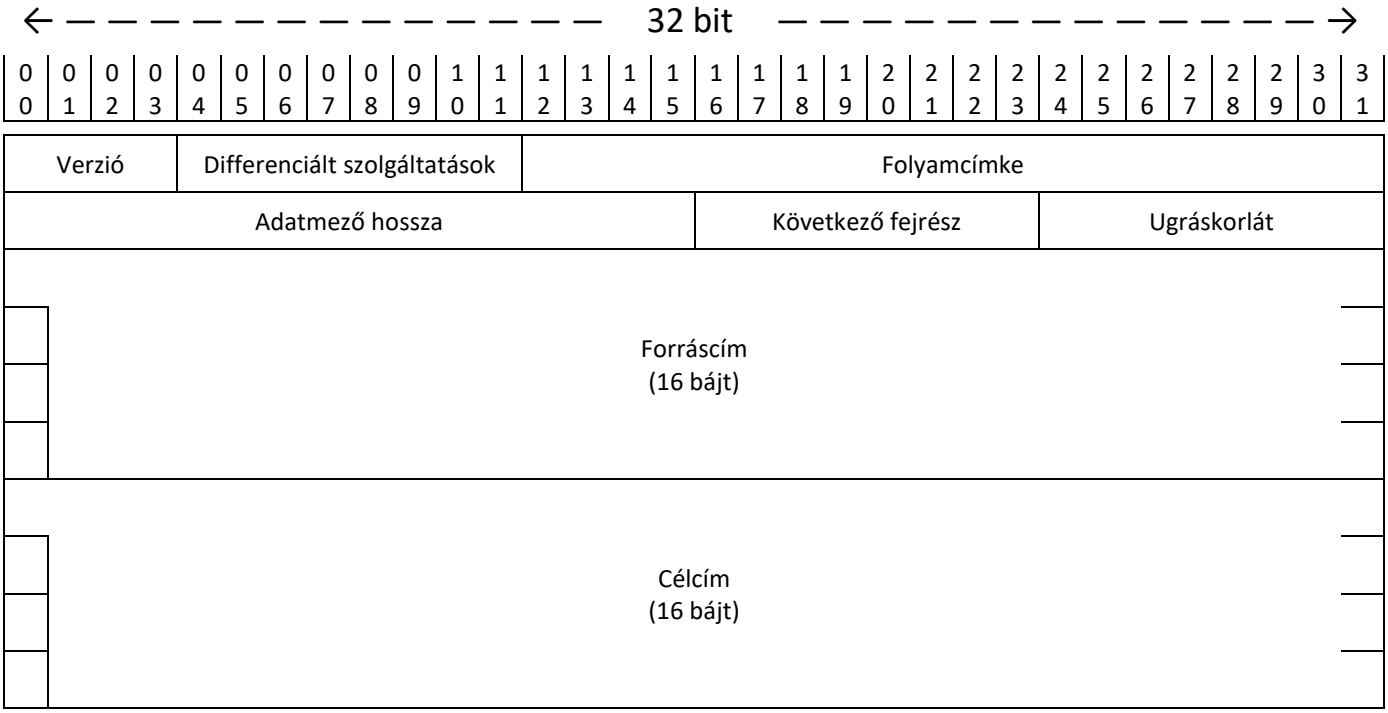
Az IPv6 legfontosabb jellemzői végül a következők lettek.

- Megnövelt, nagyobb címtartomány.
- Közvetlen végponti címezhetőség.
- Automatikus konfiguráció, vagyis a hosztok automatikus hálózati konfigurálását egy támogató rendszer végzi.
- Hálózati mobilitás, vagyis egy hálózati csatolóhoz egy időben több címet rendelhetünk. Ez hasonló a mobilszolgáltatók roaming szolgáltatásához.
- Titkosítás, azonosítás. Az IPv6 címzés szerves része az IPsec biztonsági protokoll, ez hálózati szinten nyújt lehetőséget arra, hogy a kommunikációban résztvevő felhasználók hitelesen azonosítsák egymást, és az egymás közt zajló adatforgalmat titkosítsák egy biztonságos úgynevezett alagúton (Tunnel) keresztül anélkül, hogy az Internetről bárki le tudná hallgatni őket – ez persze az elmélet, a lehallgatás a valóságban nemzetbiztonsági érdek.
- Többszörös címezhetőség, szabványosított Multicast.

Az átállás az IPv4-ről IPv6-ra nem tud az egész Interneten egy időben lezajlani, ezért szükséges, hogy a két rendszer egymás mellett működhessen, akár az Interneten vagy akár egy hoszton belül is. Ezt az átmenetet a kompatibilis címek – az IPv4 címek egyszerűen átalakíthatók IPv6-címekké – és a különféle alagutak alkalmazása biztosítja. Használható egy kettős protokollcsomag (Dual Stack IP) nevű technika is, amely mindkét protokollt egy időben támogatja. A két teljesen különálló hálózati alrendszer és a két különböző protokollverzió ebben az esetben nincs zavaró hatással egymásra.
A végfelhasználók szempontjából a legfontosabb változás az, hogy minden végfelhasználó fix IPv6 címhez juthat, azaz az IPv4-ben megismert NAT ezzel elvileg okafogyottá válik. (Nem kell üldözési mánia ahhoz, hogy belássuk, ez bizonyos szempontból hátrány is lehet…) Mivel a címtartományt az IPv6 esetében 128 bitre növelték, így több mint háromezer milliárd (2^{128} = kb. $3{,}4*10^{38}$) darab IPv6 cím osztható ki.

Az IPv6 fejrésze (IPv6 Header)

Az IPv4 ismeretében lehetőségünk van a fejrészek összehasonlításra. Az IPv6 céljai között szerepelt a protokoll egyszerűsítése, ami már a fejrészen is észrevehető. Az IPv6 fejrész csak 8 mezőt tartalmaz, az IPv4 fejrész viszont 13 mezőt, és bár az IPv6 címek 16 bájtosak, mégis – a kiegészítő fejrészek nélkül összehasonlítva – csupán dupla olyan hosszú, mint a régi IPv4 fejrész. Maga az IPv6 cím továbbra is 32 bites szavakból áll, pontosan 10 ilyen szóból, tehát a hossza 320 bit, azaz 40 bájt.



Az IPv6 fejrész mezői a következők:

- Verzió: IPv6 esetében értéke 6.
- A differenciált szolgáltatások a második mező – eredetileg forgalmi osztály (Traffic Class) volt a mező neve, érdekes hogy már az IPv4 esetében ennél a mezőnél volt névcsere… Funkciója is az IPv4-ben megismert, azaz az első 2 bit az explicit torlódás jelzésére szolgál, az utolsó 6 bit pedig prioritási szinteket jelez.
- A folyamcímke (Flow Label) vagy folyam azonosító alkalmas az ugyanattól a feladó hoszttól ugyanaddig a vevő hosztig futó logikailag egybetartozó csomagok megjelölésére. Így az egybe tartozó csomagoknak – folyamoknak – egyedi sávszélességbeli vagy késleltetési igénye lehet. Például egy TCP kapcsolat lehet egy folyam. A folyamcímke 0 értéke pedig azt jelzi, hogy a csomag nem tartozik egyetlen folyamhoz sem. A módszer lehetőséget teremt a datagram alapú hálózat rugalmasságának és a virtuálisáramkör alapú hálózat garanciáinak ötvözésére. A folyamcímke leírását az RFC1809 dokumentum tartalmazza.

- Az adatmező hossza mező mondja meg, hogy a fejrész 40 bájtja után mennyi adatbájt következik. Fontos változás, hogy az adatmező hosszában az IPv6 esetében a fejrész már nem számít bele a hosszba. Így a rendelkezésre álló 16 bit segítségével az adatmező hossza maximum 65535 bájt lehet.
- A következő fejrész mező arra utal, hogy az IPv6 fejrész után további fejrészek is következhetnek, melyek az IPv4-ben még opciók voltak. A kiegészítő fejrészek formátuma eltér az IPv6 fejrész formátumától, azaz specifikus mezőket tartalmaznak. Jelenleg 8 fajta ilyen további fejrész következhet. Ezen fejrészek sorrendje kötött. Minden fejrész tartalmazza a következő fejrész típusát, kivéve az utolsót (ami a felsőbb rétegek fejrésze, mivel a sorrend is kötött). Minden fejrészben benne van, hogy mit kell tennie annak az útválasztónak, aki nem ismeri fel az egyes fejrészeket. A lehetőségek: dobja el, továbbítsa, vagy küldjön a feladónak ICMP üzenetet. A sorban elöl a minden ugrás által feldolgozandó fejrész van, majd a közbülső- illetve a végpontok által feldolgozandó fejrészek következnek, végül pedig a felsőbb rétegekben feldolgozandó fejrész a zárja a sort.
    1. Hop-by-Hop Options header
       Egyetlen opciója a Jumbogram, azaz a 64kB-nál nagyobb datagramok támogatása, amit minden érintett útválasztónak fel kell tudnia dolgozni.
    2. Destination Options header (első előfordulás)
       Az egyetlen opció, mely kétszer is előfordulhat. Ebben a pozícióban a közbülső állomások számára tartalmaz adatokat.
    3. Routing header
       Az IPv4 szerinti forrás általi útválasztás (Source Routing Option) megfelelője, azaz a laza vagy szigorú útválasztást, útvonaljelölést tartalmazza.
    4. Fragment header
       A csomag tördelésével kapcsolatos információkat tartalmazza. Közbülső útválasztók részére tilthatja vagy engedélyezheti a csomagdarabolást.
    5. Authentication header
       Hitelesítési azaz autentikációs információkat tartalmaz. Segítségével ellenőrizhető, hogy valóban a küldő küldte-e, illetve, hogy történt-e változás az adatokban az átvitel során.
    6. Encrypted Security Payload header
       Célja a titkosítás, azaz hogy csak a valódi címzett tudja az adatokat elolvasni.
    7. Destination Options header (második előfordulás)
       Ebben a pozícióban csak a célállomás számára tartalmaz információkat.
    8. Upper Layer Header
       A célállomás felsőbb rétegei számára tartalmaz információkat.

- Az ugráskorlát mező funkciója az IPv4 TTL mező funkcióhoz hasonlít. Feladata, hogy a csomagok élettartamát ugrásonként csökkentse. A csökkentésnek az IPv6 esetében időhöz nem, csak az ugrások számához van köze – erre utal az elnevezés megváltoztatása is.
- A forráscím mező hossza 16 bájt, és a küldő hoszt címét tartalmazza.
- A célcím mező hossza 16 bájt, és a cél hoszt címét tartalmazza.

Amit mindenképpen illik észrevenni – mint változást az IPv4-hez képest – az a darabolással kapcsolatos mezők és az ellenőrző összeg mező eltűnése.
A csomagdarabolás filozófiájában történt a változtatás, ugyanis az IPv6 esetében sokkal kevésbé preferált az csomagok út közbeni, azaz útválasztók általi darabolása. A preferált módszer az útvonal MTU-jának gyors felderítése után az eleve megfelelő méretű csomagok előállítása.
Az ellenőrző összeget – ami az IPv4-ben főleg a TTL-nek köszönhetően amúgy is bonyolult, ezáltal az egész átvitelre nézve lassító (erőforrás elvonó) hatású volt – azért lehetett elhagyni, mert egyrészt a hálózatok megbízhatósága a hálózatok evolúciója során sokat javult, illetve indokolatlanná is vált, hiszen a szállítási rétege amúgy is rendelkezik ellenőrző összeggel.

Az IPv6 címek

Az IPv6 címzési rendszere nem tartalmaz az IPv4-ben megismert osztályokat. Egy 16 bájtos címnek pusztán a leírása is komoly feladat, ezért többféle ábrázolásmód van használatban.

- Leírhatjuk az IPv6 címet 8 db, egyenként 4 db hexadecimális szám kettősponttal elválasztott sorozataként:
  8000:0000:0000:0000:0123:4567:89AB:CDEF
- A hatalmas címtartomány sok esetben tartalmaz sok egymás utáni „0” értéket. A „0”-ák elhagyására két egyszerűsítés létezik. Egyrészt a felvezető „0”-kat hagyhatjuk el (egy címben ezt csak egy alkalommal engedi a szabvány), a másrészt a csak „0”-ákból álló csoportokat hagyhatjuk el:
  8000:0:0:0:123:4567:89AB:CDEF
  8000::123:4567:89AB:CDEF
- A régi (IPv4) címe írásmódja viszont maradt decimális, azaz a következő:
  ::192.168.50.25
- A hálózati maszkot kizárólag a prefix értéke jelöli:
  8000::123:4567:89AB:CDEF/64

A fontosabb nevezetes címtartományok, címcsoportok.

- Reserved by IETF — Az IETF által szabványba rögzítetten lefoglalt tartományok.
  http://www.iana.org/assignments/ipv6-address-space/ipv6-address-space.xhtml
- ::/128 — Unspecified Address
  A hosztok inicializálásakor használatos, végig nullákból áll.
- ::/0 — Alapértelmezett Unicast átjárócím.
- ::1/128 — Loopback Address
  A visszacsatolásos tesztelés címtartománya.
- ::/96 — IPv4 Compatible IPv6 Address
  Ma már nincs érvényben, mert az IPv4 – IPv6 átmenetre született jobb (éppen a soron következő) megoldás.
- ::FFFF:0:0/96 — Az IPv4 – IPv6 átmenetre fenntartott tartomány.
- 2000::/3 — Global Unicast
- FC00::/7 — Unique Local Unicast
  A privát címek tartománya, melyek olyan helyeken is használhatóak, ahol nincs hivatalosan kiosztott IPv6 prefix. (RFC4139)
- FE80::/10 — Link-Local Unicast
  Olyan címek tartománya, melyek csak egy adott fizikai link-en, például szegmensen érvényesek. (RFC4862)
- FEC0::/10 — Site-Local Unicast
  Olyan címek tartománya, melyek csak egy Site-on belül érvényesek. Nincs használatban, mert a Site fogalma sem pontosan meghatározott. (RFC3978)
- FF00::/8 — Multicast
  Broadcast és Multicast céljára felhasználható címek tartománya.

Az NDP protokoll

A korábban megismert ARP által megvalósított funkció (az IPv4 és a MAC címek összerendelése) az IPv6 esetében számos további funkcióval kiegészítve, szomszéd felismerő protokoll (NDP – Neighbour Discovery Protocol) néven működik.
A környezet felismerő protokoll a hálózatban elhelyezkedő aktív hálózati eszközök, entitások (hosztok, útválasztók) feltérképezésére szolgál. Információt szolgáltat az útválasztóknak, hosztnak a környezetükben található hálózati eszközök elérhetőségéről, céméről. Az NDP leírását az RFC4861 dokumentum tartalmazza.

A protokoll feladatai a következők:

- Útválasztó felderítése (Router Discovery)
  Ez egy eljárás a hosztok számára, arról, hogy hogyan deríthetik fel a hálózathoz kapcsolódó útválasztókat.
- Cím előtagjának felderítése (Prefixr Discovery)
  Ez egy eljárás a hosztok számára, arról, hogy képesek legyenek a cím előtag beállítására.
- Paraméter felderítés (Parameter Discovery)
  Ez egy eljárás a hosztok számára, arról, hogy honnan szerezhetnek tudomást az egyes paraméterekről, mint például a kapcsolatparaméterekről – például MTU, vagy az Internet paramétereiről – például. hogy hány pontot érinthet maximálisan az útja során a csomag (Hop Limit)
- Automatikus címkonfigurálás (Address Autoconfiguration)
  Ez egy eljárás a hosztok számára, arról, hogy hogyan végezhetik el az egyes kapcsolódási pontok címének automatikus konfigurálását.
- Cím feloldás (Address resolution)
  Ez egy eljárás a hosztok számára, arról, hogy hogyan határozhatják meg az IP cím ismeretében a fizikai címet.
- Következő ugrás meghatározása (Next-hop determination)
  Ez egy algoritmus, amely leképezi a cél IP címét annak a csomóponti hosztnak a címére, ahova a csomagot továbbítani kell. Ez lehet maga a célpont vagy egy közbülső útválasztó.
- Elérhetetlen szomszéd érzékelés (Neighbor Unreachability Detection)
  Ez egy módszer arra, hogy a hosztok hogyan érzékelhetik, ha valamelyik, velük egy hálózaton levő hálózati eszköz elérhetetlenné válik.

- Cím ismétlődés érzékelése (Duplicate Address Detection)
  Ez egy eljárás a hosztok számára, arról, hogy hogyan érzékelhetik azt, hogy az általuk használni kívánt címet használja-e valamely más hálózati eszköz.
- Átirányítás (Redirect)
  Ez egy eljárás az útválasztók számára arról, hogy hogyan tudja értesíteni a hosztokat arról, hogy létezik az általa eddig használtnál jobb (gazdaságosabb) csomagküldési útvonal is.

Az NDP protokoll, mivel az IPv6 protokoll része, ICMPv6 csomagokat felhasználva oldja meg a feladatait. Az IPv6 természetesen tartalmazza az összes IPv4 által használt ICMP üzenetet is. A környezet felmérés céljaira az ICMPv6 ötféle üzenetet használ.

- Útválasztó kérelmezés (Router Solicitation)
- Útválasztó hirdetés (Router Advertisements)
- Szomszéd kérelmezés (Neighbor Solicitation)
- Szomszéd hirdetés (Neighbor Advertisements)
- Átirányítás (Redirect)